Active Directory Tech Team

Report and recommendations

AD Tech Team

- Members from SITSD, DOJ, DPHHS, LEG, DLI, DOR, OPI, & MDT
- Charged with reviewing current AD structure and architecture.
- Three phases
  - Phase 1 – Active Directory Health Checks
  - Phase 2 – Microsoft AD review and report
  - Phase 3 – Evaluation of Microsoft AD report to choose one of the options presented as path forward.

AD Tech Team Phase 1 & 2

- Phase 1 – AD Health checks on Enterprise forest, DOJ, and DPHHS.
  - Minor issues found with all three forests.
- Phase 2 – Microsoft AD review and report
  - Microsoft interviews of agencies and current use of AD within agencies and Enterprise
  - Report presented four options

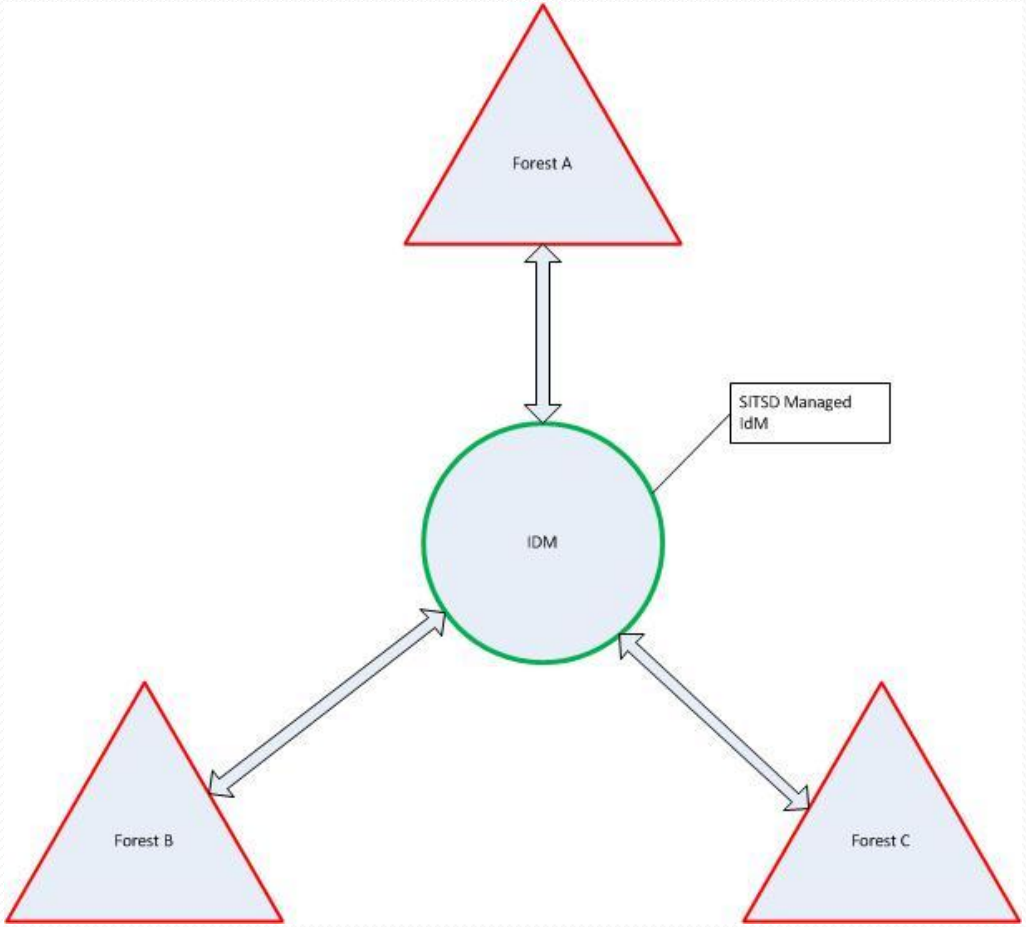
Microsoft Options

- Option 1 – No change to current operations. Continue with no trusts and no identity management
- Option 2 – Consolidate to a single forest and domain for the entire enterprise.
- Option 3 – Decentralize Active Directory to agency based forests with no IDM or connections
- Option 4 – Establish trusts and/or identity management connections between the existing AD forests
- Option 5 (presented by HHS) – Similar to 4 with agency managed IdM solutions.

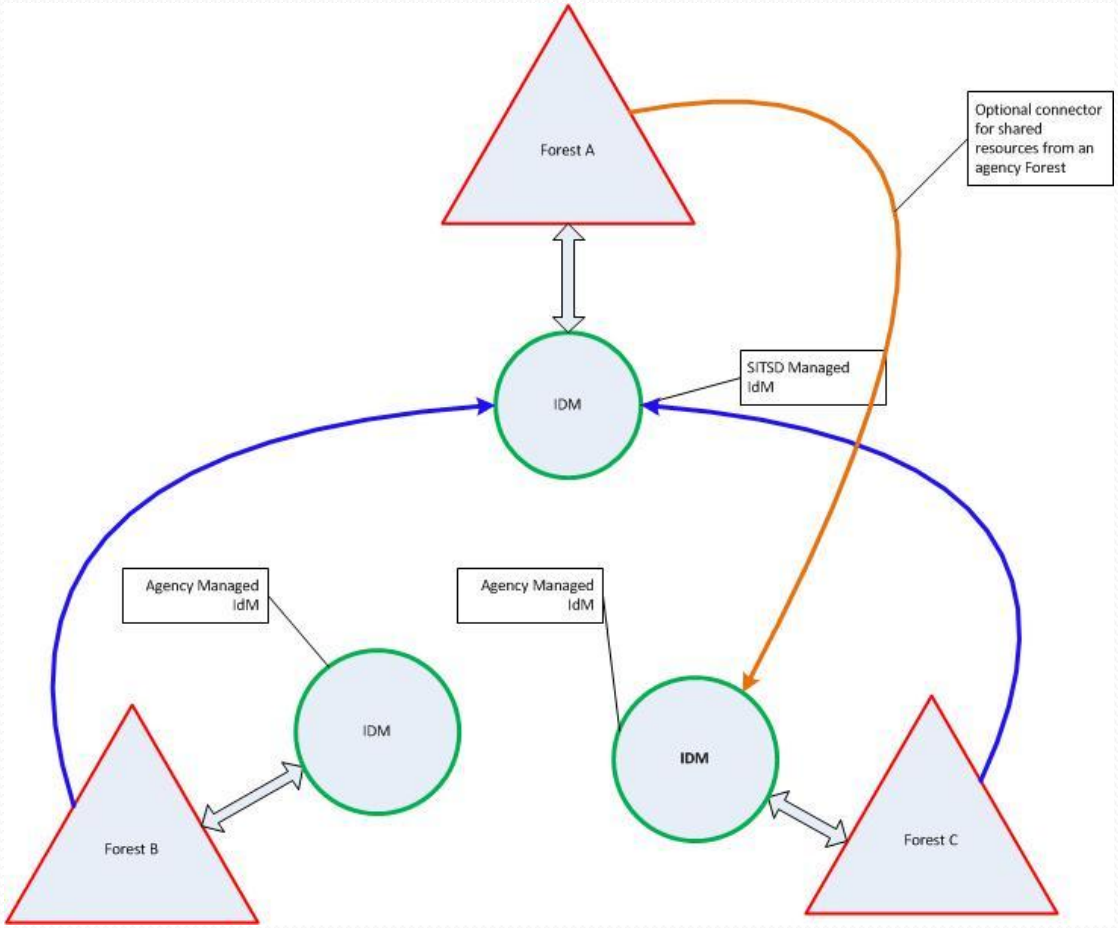
AD Business requirements

- Business requirements were extremely difficult to define across multiple agencies, all with unique needs.
  - Requirements became a mix of technical and business needs.
  - Concept was to evaluate the options against each business requirement.
- Effort was refocused in December to concentrate on evaluation of Options presented by Microsoft.
  - Each agency presented which option was their preference.
  - In December Options 1, 2, & 3 were determined by the team not to be feasible and the team would concentrate on option 4 & 5.

Option 4 - Multiple AD with single IdM



Option 5 – Multiple AD with multiple IdM solutions



AD Team Technical Architecture recommendations

- Authentication and Authorization directory of choice should be Active Directory.
- The state needs an IdM solution(s) to facilitate cross-agency information sharing.
- Need to provide a single LDAP directory for SABHRS, FileNet, & other LDAP based applications.
- Consensus of the agency team members was Option 5.
  - Greatest agency flexibility
  - Allows for agency control of both directory and IdM solution.
- SITSD preference is Option 4.
  - Lower cost than Option 5.
  - Lower implementation complexity

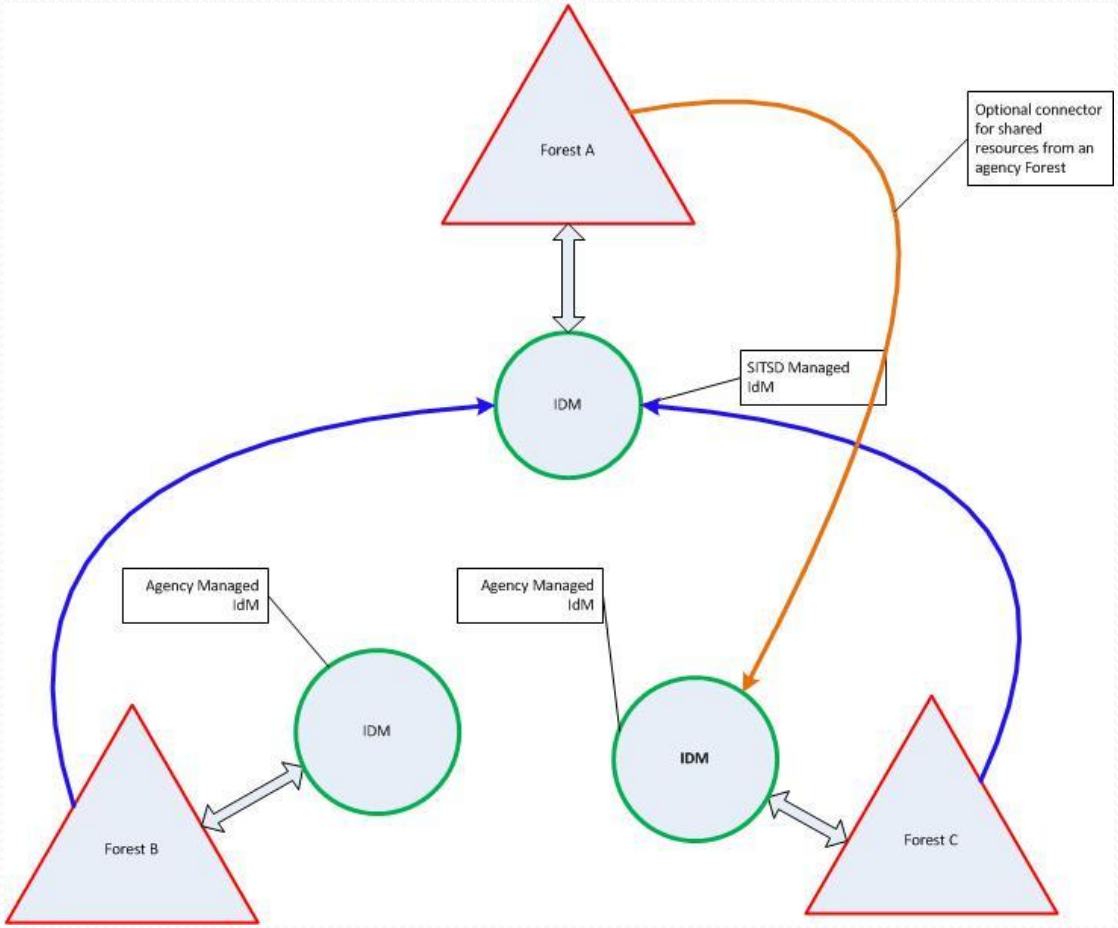
Overall Team recommendations

- The state should move forward to:
  - Establish Active Directory trust relationships between the existing AD forests. (Technical details and design to be established)
  - Investigate and Procure an IdM solution to allow interfaces to be developed between the Enterprise AD forest and agency forests.

AD Future – SITSD Perspective

- Enterprise forest with majority of agency user ID's, resources, and a single IdM solution.
- The Enterprise IdM solution forms the basis for the single LDAP user directory store.
- The Enterprise Forest interfaces with agency run forests and agency run IdM solutions in known and controlled manner. The interfaces are provided on a cost basis.
- Agencies have the ability to establish authentication and IdM solutions on their own however they will bear the full implementation and integration cost of those solutions.

AD Future


Forest A
Optional connector for shared resources from an agency Forest
IDM
SITSD Managed IdM
Agency Managed IdM
Agency Managed IdM
IDM
IDM
Forest B
Forest C

AD Future Expanded